UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/790,082	03/02/2004	Takeo Yoshida	118918	2490

25944 7590 12/09/2008

OLIFF & BERRIDGE, PLC
P.O. BOX 320850
ALEXANDRIA, VA 22320-4850

EXAMINER	
LOUIE, OSCAR A	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
12/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/790,082	YOSHIDA, TAKEO	
	Examiner	Art Unit	
	OSCAR A. LOUIE	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 September 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5-7 and 9-18* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5-7 and 9-18* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This second non-final action is in response to the amendment filed 09/09/2008. Claims 1-3, 5-7, & 9-18 are pending and have been considered as follows.

Specification

1. The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required:

- Claim 1:
  - Line 26 recites "independent of the authentication server" however, this limitation lacks antecedent basis in view of the applicant's Specification;
- Claim 5:
  - Lines 6 & 8 recite "independent of the authentication server" however, this limitation lacks antecedent basis in view of the applicant's Specification;
- Claim 6:
  - Line 24 recites "independent of the authentication server" however, this limitation lacks antecedent basis in view of the applicant's Specification;
- Claim 7:
  - Lines 16-18 recite "independent of the authentication server" however, this limitation lacks antecedent basis in view of the applicant's Specification;

- Claim 10:
    - Lines 6 & 7 recite "independent of the authentication server" however, this limitation lacks antecedent basis in view of the applicant's Specification;
- Claim 13:
    - Lines 28 & 35 recite "independent of the authentication server" however, this limitation lacks antecedent basis in view of the applicant's Specification;
- Claim 15:
    - Lines 4-6 recite "independent of the authentication server" however, this limitation lacks antecedent basis in view of the applicant's Specification;
- Claim 17:
    - Lines 4-6 recite "independent of the authentication server" however, this limitation lacks antecedent basis in view of the applicant's Specification;
- Claim 18:
    - Lines 2, 5, 11, & 21 recite "independent of the authentication server" however, this limitation lacks antecedent basis in view of the applicant's Specification;

Claim Objections

2. Claims 1, 3, 5-7, 9, 12, & 18 are objected to because of the following informalities:

- Claim 1:
  - Lines 6, 10, 15, 19, 22, 24, 29, & 32 recite the term "for" which should be "…configured to…" as the current claim language appears to be intended use language;
  - Line 13 recites the term "when" which should be "...once..." to clarify exactly "when" the limitation which precedes it occurs;
- Claim 3:
  - Line 1 recites "for being" which should be omitted as the current claim language appears to be intended use language;
  - Lines 4, 8, & 11 recite the term "for" which should be "…configured to…" as the current claim language appears to be intended use language;
  - Line 9 recites the term "when" which should be "...once..." to clarify exactly "when" the limitation which precedes it occurs;
- Claim 5:
  - Lines 3 & 10 recite the term "for" which should be "…configured to…" as the current claim language appears to be intended use language;

- Claim 6:
    - Lines 6, 10, 14, 20, & 23 recite the term "for" which should be "…configured to…" as the current claim language appears to be intended use language;
    - Line 11 recites the term "when" which should be "...once..." to clarify exactly "when" the limitation which precedes it occurs;
- Claim 7:
    - Lines 4, 8, & 12 recite the term "for" which should be "…configured to…" as the current claim language appears to be intended use language;
    - Line 5 recites the term "for" which should be omitted as the current claim language appears to be intended use language;
    - Line 9 recites the term "when" which should be "...once..." to clarify exactly "when" the limitation which precedes it occurs;
- Claim 9:
    - Lines 3, 6, 10, & 14 recite the term "for" which should be "…configured to…" as the current claim language appears to be intended use language;
    - Line 21 recites the term "when" which should be "...if..." to clarify exactly "when" the limitation which precedes it occurs;
    - Lines 3-5 and lines 19-22 appear to be very similar, where lines 19-22 appear to include additional details not found in lines 3-5, the examiner suggests consolidation of these two sets of limitations in order to avoid unnecessary redundancy and improve claim clarity;

- Claim 12:
    - Line 7 recites "associating" which in keeping with the nature of the other amendments, appears to have been meant to be written as "…storing…";
    - Lines 13 & 16 recite the term "when" which should be "...once..." to clarify exactly "when" the limitation which precedes it occurs;
- Claim 18:
    - Line 1 recites "computer readable medium" which should be "…computer readable storage medium…";
    - Line 27 recites the term "when" which should be "...if..." to clarify exactly "when" the limitation which precedes it occurs;
- See MPEP 2106 with respect to intended use or other similar language as necessary:

> *The subject matter of a properly construed claim is defined by the terms that limit its scope. It is this subject matter that must be examined. As a general matter, the grammar and intended meaning of terms used in a claim will dictate whether the language limits the claim scope. Language that suggests or makes optional but does not require steps to be performed or does not limit a claim to a particular structure does not limit the scope of a claim or claim limitation. The following are examples of language that may raise a question as to the limiting effect of the language in a claim:*
> *(A) statements of intended use or field of use,*
> *(B) "adapted to" or "adapted for" clauses,*
> *(C) "wherein" clauses, or*
> *(D) "whereby" clauses.*

Appropriate correction is required.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 1, 5-7, 10, 13, 15, 17, & 18 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

- Claim 1:
    - Line 26 recites "independent of the authentication server" however, this limitation appears to lack support in view of the applicant's original disclosure and is thereby considered as new matter;
- Claim 5:
    - Lines 6 & 8 recite "independent of the authentication server" however, this limitation appears to lack support in view of the applicant's original disclosure and is thereby considered as new matter;
- Claim 6:
    - Line 24 recites "independent of the authentication server" however, this limitation appears to lack support in view of the applicant's original disclosure and is thereby considered as new matter;

- Claim 7:
    - Lines 16-18 recite "independent of the authentication server" however, this limitation appears to lack support in view of the applicant's original disclosure and is thereby considered as new matter;
- Claim 10:
    - Lines 6 & 7 recite "independent of the authentication server" however, this limitation appears to lack support in view of the applicant's original disclosure and is thereby considered as new matter;
- Claim 13:
    - Lines 28 & 35 recite "independent of the authentication server" however, this limitation appears to lack support in view of the applicant's original disclosure and is thereby considered as new matter;
- Claim 15:
    - Lines 4-6 recite "independent of the authentication server" however, this limitation appears to lack support in view of the applicant's original disclosure and is thereby considered as new matter;
- Claim 17:
    - Lines 4-6 recite "independent of the authentication server" however, this limitation appears to lack support in view of the applicant's original disclosure and is thereby considered as new matter;

- Claim 18:
    - Lines 2, 5, 11, & 21 recite "independent of the authentication server" however, this limitation appears to lack support in view of the applicant's original disclosure and is thereby considered as new matter;

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 12 & 18 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

- Claim 12 discloses "a connection method using a network connection system including a client apparatus, an authentication server, and a connection server" comprising several steps, however, it is unclear and difficult to determine which "server" or "apparatus" performs which step;
- Claim 18 discloses "a computer readable medium storing a program causing a computer of a client apparatus to execute an access processing to a network system including an authentication server and a connection server" however, it is unclear as to at which point the client apparatus receives and stores, if ever, the first and second information generated by the connection server;

Claim Rejections - 35 USC § 101

7. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1, 3, 5-7, 9-11 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

- Claim 1 discloses "a network connection system" comprising "a client apparatus" and "authentication server" and "a connection server" however, these three components of the system appear to be merely software; that is, there does not appear to be supporting evidence in view of the applicant's Specification or Drawings that would clearly illustrate or disclose that these components are hardware apparatuses and not merely computer software programs, thereby invoking 35 U.S.C. 101 as non-statutory subject matter;
- Claim 3 discloses "an authentication server for being connected to a plurality of client apparatuses and a plurality of connection servers" comprising a plurality of "units" which appear to be nothing more than computer software programs, thereby invoking 35 U.S.C. 101 as non-statutory subject matter;
- Claim 5 discloses "a connection server operating with an authentication server and a client apparatus" comprising a plurality of "units" which appear to be nothing more than computer software programs, thereby invoking 35 U.S.C. 101 as non-statutory subject matter;
- Claim 6 discloses "a network connection system" comprising "a client apparatus" and "an authentication server" and "a connection server" however, these three components of the system appear to be merely software with each comprising a plurality of "units"

which also appear to be nothing more than computer software programs, thereby invoking 35 U.S.C. 101 as non-statutory subject matter;

- Claim 7 discloses "an authentication server operating with a plurality of client apparatuses and a plurality of connection servers" comprising a plurality of "units" which appear to be nothing more than computer software programs, thereby invoking 35 U.S.C. 101 as non-statutory subject matter;
- Claim 9 discloses "a client apparatus operating with an authentication server and a connection server" comprising a plurality of "units" which appear to be nothing more than computer software programs, thereby invoking 35 U.S.C. 101 as non-statutory subject matter;
- Claim 10 discloses "a connection server operating with a client apparatus and an authentication server" comprising a plurality of "units" which appear to be nothing more than computer software programs, thereby invoking 35 U.S.C. 101 as non-statutory subject matter;
- Claim 11 discloses "a network connection system" comprising "a client apparatus" and "authentication server" and "a connection server" however, these three components of the system appear to be merely software; that is, there does not appear to be supporting evidence in view of the applicant's Specification or Drawings that would clearly illustrate or disclose that these components are hardware apparatuses and not merely computer software programs, thereby invoking 35 U.S.C. 101 as non-statutory subject matter;

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 5, 10, & 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fuh et al. (US-6463474-B1).

Claims 5 & 15:

Fuh et al. disclose a connection server operating with an authentication server and a client apparatus comprising,

- "switching from a state in which authentication information is not allowed to be received from the client address, independent of the authentication server, to a state in which authentication information is allowed to be received from the client address, independent of the authentication server" (i.e. "the firewall re-configures itself, in response to successful authentication, so that packets that would otherwise be barred are now allowed to pass") [column 7 lines 58-61];
- "the switching occurring in response to the receiving of the client address" (i.e. "In response to receiving the authentication information, the firewall performs an authentication") [column 7 lines 50-51];

- "an authentication unit for receiving the authentication information from the client apparatus having the client address to perform itself an authentication process by using the authentication information" (i.e. "In response to receiving the authentication information, the firewall performs an authentication and authorization process") [column 7 lines 50-52];

but, they do not explicitly disclose,

- "a control unit for receiving a client address of the client apparatus from the authentication server after the authentication server authenticates information received from the client address," although Fuh et al. do suggest including source and destination IP addresses in the packets used in communication between devices, as recited below;
- "wherein after a limited time period has elapsed since the control unit performs the switching, the control unit switches back from the state in which authentication information is allowed to be received from the client address, independent of the authentication server, to the state in which authentication information is not allowed to be received from the client address, independent of the authentication server," although Fuh et al. do suggest switching modes/states, as recited below;

however, Fuh et al. do disclose,

- "Each packet of an HTTP request includes a header portion that contains one or more fields of information. The fields include, among other things, values for source IP address and destination IP address of that packet" [column 10 lines 23-24];
- "the firewall re-configures itself, in response to successful authentication, so that packets that would otherwise be barred are now allowed to pass") [column 7 lines 58-61];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a control unit for receiving a client address of the client apparatus from the authentication server after the authentication server authenticates information received from the client address" and "wherein after a limited time period has elapsed since the control unit performs the switching, the control unit switches back from the state in which authentication information is allowed to be received from the client address, independent of the authentication server, to the state in which authentication information is not allowed to be received from the client address, independent of the authentication server," in the invention as disclosed by Fuh et al. for the purposes of providing adjustable access control based on the source and destination address of sent and received information.

Claim 10:

Fuh et al. disclose a connection server operating with an authentication server and a client apparatus comprising,

- "switches, in response to the receiving of the address, from a state in which authentication information is not allowed to be received from the client address, independent of the authentication server, to a state in which authentication information is allowed to be received from the client address, independent of the authentication server" (i.e. "the firewall re-configures itself, in response to successful authentication, so that packets that would otherwise be barred are now allowed to pass") [column 7 lines 58-61];

- "allows communication from the address of the client apparatus for a predetermined period" (i.e. "the firewall re-configures itself, in response to successful authentication, so that packets that would otherwise be barred are now allowed to pass") [column 7 lines 58-61];
- "a transmitting unit that transmits to the authentication server information indicating that the connection server has shifted to a connection wait state in which the connection server allows communication from the address of the client apparatus for the predetermined period" (i.e. "the firewall re-configures itself, in response to successful authentication, so that packets that would otherwise be barred are now allowed to pass") [column 7 lines 58-61];

but, they do not explicitly disclose,

- "a control unit that receives from the authentication server an address of the client apparatus and," although Fuh et al. do suggest including source and destination IP addresses in the packets used in communication between devices, as recited below;

however, Fuh et al. do disclose,

- "Each packet of an HTTP request includes a header portion that contains one or more fields of information. The fields include, among other things, values for source IP address and destination IP address of that packet" [column 10 lines 23-24];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a control unit that receives from the authentication server an address of the client apparatus and," in the invention as disclosed by Fuh et al. for the purposes of providing adjustable access control based on the source and destination address of sent and received information.

10. Claims 1-3, 6, 7, 9, 11-14, 16, & 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lander (US-7350229-B1) in view of Fuh et al. (US-6463474-B1).

Claims 1:

Lander discloses a network connection system comprising,

- "a client apparatus" (i.e. "a client") [column 8 line 45];
- "an authentication server" (i.e. "front-end server") [column 8 line 45];
- "a connection server" (i.e. "back-end content servers") [column 8 line 66];
- "the authentication server includes: a retention unit for storing second connection authentication information generated by the connection server based on user identification information" (i.e. "memory 106, and at least one storage device") [column 8 line 47];
- "a first unit for acquiring, from the client apparatus, second connection authentication information that is generated by the client apparatus based on user identification information input into the client apparatus" (i.e. "When the user signs onto the front-end server cluster 202, the central security process 222 transmits the user login data (e.g., username and password) to the policy server 204") [column 11 lines 11-14];

- "acquiring a client address of the client apparatus when the first unit receives a connection request from the client apparatus" (i.e. "An electronic device, such as a front-end server 102 receives a client request 116") [column 8 lines 44-45];
- "the client apparatus includes: a third unit for transmitting the second connection authentication information generated by the client apparatus to the authentication server together with the connection request" (i.e. "When the user signs onto the front-end server cluster 202, the central security process 222 transmits the user login data (e.g., username and password) to the policy server 204") [column 11 lines 11-14];

but, Lander does not explicitly disclose,

- "storing an association between the second connection authentication information and a connection server address of the connection server," although Fuh et al. do suggest storing client authorization information, as recited below;
- "a second unit for transmitting the client address to the connection server address associated with the second connection authentication information acquired by the first unit," although Fuh et al. do suggest sending and receiving source and destination IP addresses in the packets transmitted, as recited below;
- "transmitting the connection server address to the client apparatus," although Fuh et al. do suggest sending and receiving source and destination IP addresses in the packets transmitted, as recited below;
- "a fourth unit for receiving the connection server address from the authentication server," although Fuh et al. do suggest sending and receiving source and destination IP addresses in the packets transmitted, as recited below;

- "a fifth unit for preparing first connection authentication information based on the user identification information input into the client apparatus," although Fuh et al. do suggest user input identification information, as recited below;
- "transmitting, independent of the authentication server, the first connection authentication information to the connection server address of the connection server," although Fuh et al. do suggest receiving transmitted authentication information, as recited below;
- "the connection server includes: a sixth unit for allowing the first connection authentication information to be received from the client apparatus, the client address being received from the authentication server," although Fuh et al. do suggest receiving transmitted authentication information, as recited below;
- "a seventh unit for performing itself an authentication process by using the first connection authentication information transmitted from the client address," although Fuh et al. do suggest performing an authentication and authorization process, as recited below;
- "the authentication server, in response to receiving the second connection authentication information from the client apparatus, searches the retention unit for the second connection authentication information to determine the connection server address associated with the second connection authentication information," although Fuh et al. do suggest verification through matching, as recited below;

however, Fuh et al. do disclose,

- "storing client authorization information at the network device" [column 3 lines 5-6];
- "The fields include, among other things, values for source IP address and destination IP address of that packet" [column 10 lines 23-24];
- "A User 302 may enter username information in Username field 504 and may enter password information in Password field 506. To communicate the username and password information to Authentication Proxy 400, the user selects a "Submit" button 508" [column 11 lines 61-66];
- "Upon intercepting the HTTP packets, the firewall requests, from the client, authentication information such as username and password" [column 7 lines 48-50];
- "In response to receiving the authentication information, the firewall performs an authentication and authorization process" [column 7 lines 50-52];
- "determining whether a source IP address of the client in the request matches information in a filtering mechanism of the network device; and if so, determining whether the source IP address matches the authorization information stored in the network device" [column 3 lines 48-52];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "storing an association between the second connection authentication information and a connection server address of the connection server" and "a second unit for transmitting the client address to the connection server address associated with the second connection authentication information acquired by the first unit" and "transmitting the connection server address to the client apparatus" and "a fourth unit for receiving the connection

server address from the authentication server" and "a fifth unit for preparing first connection authentication information based on the user identification information input into the client apparatus" and "transmitting, independent of the authentication server, the first connection authentication information to the connection server address of the connection server" and "the connection server includes: a sixth unit for allowing the first connection authentication information to be received from the client apparatus, the client address being received from the authentication server" and "a seventh unit for performing itself an authentication process by using the first connection authentication information transmitted from the client address" and "the authentication server, in response to receiving the second connection authentication information from the client apparatus, searches the retention unit for the second connection authentication information to determine the connection server address associated with the second connection authentication information," in the invention as disclosed by Lander for the purposes of providing authentication based on multiple parts of information (i.e. address information, user identity, etc).

Claim 2:

Lander and Fuh et al. disclose a network connection system, as in Claim 1, their combination further comprising,

- "the second connection authentication information is a message digest of the first connection authentication information" (i.e. "The user identifier may also be encrypted as an additional security precaution") [column 11 lines 46-48].

Claim 14:

Lander and Fuh et al. disclose a network connection system, as in Claim 1, but Lander does not explicitly disclose,

- "wherein the sixth unit of the connection server allows the first connection authentication information to be received from the client address for a limited time period," although Fuh et al. do suggest reconfiguration to permit access, as recited below;

however, Fuh et al. do disclose,

- "In this context, "open a passageway" means that the firewall re-configures itself, in response to successful authentication, so that packets that would otherwise be barred are now allowed to pass" [column 7 lines 58-61];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein the sixth unit of the connection server allows the first connection authentication information to be received from the client address for a limited time period," in the invention as disclosed by Lander for the purposes of adjusting access control for permitting access.

Claim 3:

Lander discloses an authentication server for being connected to a plurality of client apparatuses and a plurality of connection servers comprising,

- "a retention unit for storing second connection authentication information generated based on user identification information" (i.e. "memory 106, and at least one storage device") [column 8 line 47];

- "a first unit for acquiring the second connection authentication information from a client apparatus and a client address when the first unit receives a connection request from the client apparatus" (i.e. "When the user signs onto the front-end server cluster 202, the central security process 222 transmits the user login data (e.g., username and password) to the policy server 204") [column 11 lines 11-14];

but, Lander does not explicitly disclose,

- "storing an association between each second connection authentication information and a connection server address of a corresponding connection server," although Fuh et al. do suggest storing client authorization information, as recited below;
- "a second unit for transmitting the acquired client address to the connection server address of the connection server associated with the acquired second connection authentication information," although Fuh et al. do suggest sending and receiving source and destination IP addresses in the packets transmitted, as recited below;
- "transmitting, independent of the connection server, the connection server address to the client apparatus which has transmitted the connection request," although Fuh et al. do suggest sending and receiving source and destination IP addresses in the packets transmitted, as recited below;
- "wherein the authentication server, in response to receiving the second connection authentication information from the client apparatus, searches the retention unit for the second connection authentication information to determine the connection server address associated with the second connection authentication information," although Fuh et al. do suggest verification based on matching, as recited below;

however, Fuh et al. do disclose,

- "storing client authorization information at the network device" [column 3 lines 5-6];
- "The fields include, among other things, values for source IP address and destination IP address of that packet" [column 10 lines 23-24];
- "determining whether a source IP address of the client in the request matches information in a filtering mechanism of the network device; and if so, determining whether the source IP address matches the authorization information stored in the network device" [column 3 lines 48-52];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "storing an association between each second connection authentication information and a connection server address of a corresponding connection server" and "a second unit for transmitting the acquired client address to the connection server address of the connection server associated with the acquired second connection authentication information" and "transmitting, independent of the connection server, the connection server address to the client apparatus which has transmitted the connection request" and "wherein the authentication server, in response to receiving the second connection authentication information from the client apparatus, searches the retention unit for the second connection authentication information to determine the connection server address associated with the second connection authentication information," in the invention as disclosed by Lander for the purposes of providing authentication based on multiple parts of information (i.e. address information, user identity, etc).

Claim 6:

Lander discloses a network connection system comprising,

- "a client apparatus" (i.e. "a client") [column 8 line 45];
- "an authentication server" (i.e. "front-end server") [column 8 line 45];
- "a connection server" (i.e. "back-end content servers") [column 8 line 66];
- "the authentication server includes: a retention unit for storing a first encrypted user name and a first encrypted password, which are encrypted by a first encryption method" (i.e. "memory 106, and at least one storage device") [column 8 line 47];
- "a first unit for acquiring the first encrypted user name and the first encrypted password and a client address when the first unit receives a connection request from the client apparatus" (i.e. "When the user signs onto the front-end server cluster 202, the central security process 222 transmits the user login data (e.g., username and password) to the policy server 204") [column 11 lines 11-14];
- "the first encrypted user name and the first encrypted password being an identification for identifying a user of the client apparatus" (i.e. "The user identifier may also be encrypted as an additional security precaution") [column 11 lines 46-48];
- "the client apparatus includes: a third unit for transmitting to the authentication server the first encrypted user name and the first encrypted password, which are encrypted by the first encryption method together with the connection request" (i.e. "When the user signs onto the front-end server cluster 202, the central security process 222 transmits the user login data (e.g., username and password) to the policy server 204") [column 11 lines 11-14];

- "transmitting, independent of the authentication server, to the connection server address a second encrypted user name and a second encrypted password, which are generated by encrypting using a second encryption method a user name and a password input by the user" (i.e. "The user identifier may also be encrypted as an additional security precaution") [column 11 lines 46-48];

but, Lander does not explicitly disclose,

- "storing an association between a connection server address of the connection server and the first encrypted user name and first encrypted password," although Fuh et al. do suggest storing client authorization information, as recited below;
- "a second unit for transmitting the acquired client address to the connection server address associated with the user identification information," although Fuh et al. do suggest sending and receiving source and destination IP addresses in the packets transmitted, as recited below;
- "receiving from the connection server information indicating that the connection server has shifted to a connection wait state," although Fuh et al. do suggest reconfiguration to permit access, as recited below;
- "transmitting, independent of the connection server, the connection server address to the client apparatus," although Fuh et al. do suggest sending and receiving source and destination IP addresses in the packets transmitted, as recited below;
- "a fourth unit for receiving the connection server address from the authentication server," although Fuh et al. do suggest sending and receiving source and destination IP addresses in the packets transmitted, as recited below;

- "the authentication server, in response to receiving the first encrypted user name and the first encrypted password from the client apparatus, searches the retention unit for the first encrypted user name and the first encrypted password to determine the connection server address associated with the first encrypted user name and the first encrypted password," although Fuh et al. do suggest verification based on matching, as recited below;

however, Fuh et al. do disclose,

- "storing client authorization information at the network device" [column 3 lines 5-6];
- "The fields include, among other things, values for source IP address and destination IP address of that packet" [column 10 lines 23-24];
- "In this context, "open a passageway" means that the firewall re-configures itself, in response to successful authentication, so that packets that would otherwise be barred are now allowed to pass" [column 7 lines 58-61];
- "determining whether a source IP address of the client in the request matches information in a filtering mechanism of the network device; and if so, determining whether the source IP address matches the authorization information stored in the network device" [column 3 lines 48-52];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "storing an association between a connection server address of the connection server and the first encrypted user name and first encrypted password" and "a second unit for transmitting the acquired client address to the connection server address associated with the user identification information" and "receiving from the connection server information indicating that the connection server has shifted to a connection wait state" and

"transmitting, independent of the connection server, the connection server address to the client apparatus" and "a fourth unit for receiving the connection server address from the authentication server" and "the authentication server, in response to receiving the first encrypted user name and the first encrypted password from the client apparatus, searches the retention unit for the first encrypted user name and the first encrypted password to determine the connection server address associated with the first encrypted user name and the first encrypted password," in the invention as disclosed by Lander for the purposes of providing authentication based on multiple parts of information (i.e. address information, user identity, etc).

Claim 7:

Lander discloses an authentication server operating with a plurality of client apparatuses and a plurality of connection servers comprising,

- "a retention unit for storing user names and passwords, which are encrypted by a predetermined method" (i.e. "memory 106, and at least one storage device") [column 8 line 47];
- "a first unit for acquiring an acquired encrypted user name, an acquired encrypted password, and an acquired client address when the first unit receives a connection request from the client apparatus" (i.e. "When the user signs onto the front-end server cluster 202, the central security process 222 transmits the user login data (e.g., username and password) to the policy server 204") [column 11 lines 11-14];
- "the encrypted user name and password being an identification information of a user of the client apparatus" (i.e. "The user identifier may also be encrypted as an additional security precaution") [column 11 lines 46-48];

but, Lander does not explicitly disclose,

- "storing association between both of each user name and each password and a connection server address of a corresponding connection server," although Fuh et al. do suggest storing client authorization information, as recited below;
- "a second unit for transmitting the acquired client address to the connection server address associated with the acquired encrypted user name and password," although Fuh et al. do suggest sending and receiving source and destination IP addresses in the packets transmitted, as recited below;
- "receiving from the connection server information indicating that the connection server has shifted state in which authentication information is not allowed to be received from the client address, independent of the authentication server, to a state in which authentication information is allowed to be received from the client address, independent of the authentication server," although Fuh et al. do suggest reconfiguration to permit access, as recited below;
- "transmitting, independent of the connection server, the connection server address to the client apparatus, which has issued the connection request," although Fuh et al. do suggest sending and receiving source and destination IP addresses in the packets transmitted, as recited below;

- "the authentication server, in response to receiving the identification information of a user of the client apparatus from the client apparatus, searches the retention unit for the identification information of a user of the client apparatus to determine the connection server address associated with the identification information of a user of the client apparatus," although Fuh et al. do suggest verification based on matching, as recited below;

however, Fuh et al. do disclose,

- "storing client authorization information at the network device" [column 3 lines 5-6];
- "The fields include, among other things, values for source IP address and destination IP address of that packet" [column 10 lines 23-24];
- "In this context, "open a passageway" means that the firewall re-configures itself, in response to successful authentication, so that packets that would otherwise be barred are now allowed to pass" [column 7 lines 58-61];
- "determining whether a source IP address of the client in the request matches information in a filtering mechanism of the network device; and if so, determining whether the source IP address matches the authorization information stored in the network device" [column 3 lines 48-52];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "storing association between both of each user name and each password and a connection server address of a corresponding connection server" and "a second unit for transmitting the acquired client address to the connection server address associated with the acquired encrypted user name and password" and "receiving from the connection server

information indicating that the connection server has shifted state in which authentication information is not allowed to be received from the client address, independent of the authentication server, to a state in which authentication information is allowed to be received from the client address, independent of the authentication server" and "transmitting, independent of the connection server, the connection server address to the client apparatus, which has issued the connection request" and "the authentication server, in response to receiving the identification information of a user of the client apparatus from the client apparatus, searches the retention unit for the identification information of a user of the client apparatus to determine the connection server address associated with the identification information of a user of the client apparatus," in the invention as disclosed by Lander for the purposes of providing authentication based on multiple parts of information (i.e. address information, user identity, etc).

Claim 9:

Lander discloses a client apparatus operating with an authentication server and a connection server comprising,

- "a connection request unit for transmitting to the authentication server a connection request and a user name and a password which are encrypted by a first encryption method" (i.e. "When the user signs onto the front-end server cluster 202, the central security process 222 transmits the user login data (e.g., username and password) to the policy server 204") [column 11 lines 11-14];
- "encrypting by a second encryption method the user name and the password input by a user" (i.e. "The user identifier may also be encrypted as an additional security precaution") [column 11 lines 46-48];

- "a retention unit for storing local authentication information, which is previously supplied from the connection server" (i.e. "memory 106, and at least one storage device") [column 8 line 47];
- "the connection request unit transmits to the authentication server the connection request and the user name and the password which are encrypted by the first method only when the user name and the password input by the user are authenticated by the local authentication unit" (i.e. "When the user signs onto the front-end server cluster 202, the central security process 222 transmits the user login data (e.g., username and password) to the policy server 204") [column 11 lines 11-14];

but, Lander does not explicitly disclose,

- "a receiving unit for receiving, independent of the connection server, a connection server address from the authentication server," although Fuh et al. do suggest sending and receiving source and destination IP addresses in the packets transmitted, as recited below;
- "a transmitting unit for transmitting the encrypted user name and password to the connection server address," although Fuh et al. do suggest receiving transmitted authentication information, as recited below;
- "the local authentication information associating unique information of the client apparatus with at least one of a user name and a password previously provided to the connection server," although Fuh et al. do suggest storing client authorization information, as recited below;

- "a local authentication unit for generating the unique information upon receiving a user name and a password input by the user," although Fuh et al. do suggest user input identification information, as recited below;
- "authenticating the user name and the password input by the user by judging based on the local authentication information whether or not at least one of the user name and the password input by the user is associated with the unique information," although Fuh et al. do suggest performing an authentication and authorization process, as recited below;

however, Fuh et al. do disclose,

- "The fields include, among other things, values for source IP address and destination IP address of that packet" [column 10 lines 23-24];
- "Upon intercepting the HTTP packets, the firewall requests, from the client, authentication information such as username and password" [column 7 lines 48-50];
- "storing client authorization information at the network device" [column 3 lines 5-6];
- "A User 302 may enter username information in Username field 504 and may enter password information in Password field 506. To communicate the username and password information to Authentication Proxy 400, the user selects a "Submit" button 508" [column 11 lines 61-66];
- "In response to receiving the authentication information, the firewall performs an authentication and authorization process" [column 7 lines 50-52];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a receiving unit for receiving, independent of the connection server, a connection server address from the authentication server" and "a transmitting unit for

transmitting the encrypted user name and password to the connection server address" and "the local authentication information associating unique information of the client apparatus with at least one of a user name and a password previously provided to the connection server" and "a local authentication unit for generating the unique information upon receiving a user name and a password input by the user" and "authenticating the user name and the password input by the user by judging based on the local authentication information whether or not at least one of the user name and the password input by the user is associated with the unique information," in the invention as disclosed by Lander for the purposes of providing authentication based on multiple parts of information (i.e. address information, user identity, etc).

Claim 11:

Lander discloses a network connection system comprising,

- "a client apparatus" (i.e. "a client") [column 8 line 45];
- "an authentication server for supplying information guiding a connection destination to the client apparatus" (i.e. "front-end server") [column 8 line 45];
- "a connection server" (i.e. "back-end content servers") [column 8 line 66];
- "if authentication is successful, encrypts the second authentication information by a first encryption method" (i.e. "The user identifier may also be encrypted as an additional security precaution") [column 11 lines 46-48];
- "transmits the encrypted second authentication information to the authentication server" (i.e. "When the user signs onto the front-end server cluster 202, the central security process 222 transmits the user login data (e.g., username and password) to the policy server 204") [column 11 lines 11-14];

but, Lander does not explicitly disclose,

- "wherein the client apparatus: calculates first authentication information unique to the client apparatus to register the first authentication information in the connection server," although Fuh et al. do suggest storing client authorization information, as recited below;
- "acquires local authentication information from the connection server," although Fuh et al. do suggest storing client authorization information, as recited below;
- "the local authentication information associating the first authentication information with a predetermined authentication information and second authentication information with the predetermined authentication information," although Fuh et al. do suggest storing client authorization information, as recited below;
- "stores the local authentication information," although Fuh et al. do suggest storing client authorization information, as recited below;
- "receives second authentication information input by a user when the user instructs a connection request with respect to the connection server," although Fuh et al. do suggest receiving transmitted authentication information, as recited below;
- "again calculates the first authentication information unique to the client apparatus," although Fuh et al. do suggest receiving transmitted authentication information, as recited below;
- "authenticates the second authentication information and the again calculated first authentication information based on the stored local authentication information," although Fuh et al. do suggest verification based on matching, as recited below;

- "receives, independent of the connection server, from the authentication server a connection server address of the connection server," although Fuh et al. do suggest sending and receiving source and destination IP addresses in the packets transmitted, as recited below;
- "transmits to the connection server address the second authentication information encrypted by a second encryption method," although Fuh et al. do suggest sending and receiving source and destination IP addresses in the packets transmitted, as recited below;
- "starts communication with the connection server," although Fuh et al. do suggest permitting access, as recited below;

however, Fuh et al. do disclose,

- "storing client authorization information at the network device" [column 3 lines 5-6];
- "Upon intercepting the HTTP packets, the firewall requests, from the client, authentication information such as username and password" [column 7 lines 48-50];
- "A User 302 may enter username information in Username field 504 and may enter password information in Password field 506. To communicate the username and password information to Authentication Proxy 400, the user selects a "Submit" button 508" [column 11 lines 61-66];
- "determining whether a source IP address of the client in the request matches information in a filtering mechanism of the network device; and if so, determining whether the source IP address matches the authorization information stored in the network device" [column 3 lines 48-52];

- "The fields include, among other things, values for source IP address and destination IP address of that packet" [column 10 lines 23-24];
- "In this context, "open a passageway" means that the firewall re-configures itself, in response to successful authentication, so that packets that would otherwise be barred are now allowed to pass" [column 7 lines 58-61];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein the client apparatus: calculates first authentication information unique to the client apparatus to register the first authentication information in the connection server" and "acquires local authentication information from the connection server" and "the local authentication information associating the first authentication information with a predetermined authentication information and second authentication information with the predetermined authentication information" and "stores the local authentication information" and "receives second authentication information input by a user when the user instructs a connection request with respect to the connection server" and "again calculates the first authentication information unique to the client apparatus" and "authenticates the second authentication information and the again calculated first authentication information based on the stored local authentication information" and "receives, independent of the connection server, from the authentication server a connection server address of the connection server" and "transmits to the connection server address the second authentication information encrypted by a second encryption method" and "starts communication with the connection server," in the invention as disclosed by Lander for the purposes of providing authentication based on multiple parts of information (i.e. address information, user identity, etc).

Claims 12 & 16:

Lander discloses a connection method using a network connection system including a client apparatus, an authentication server, and a connection server comprising,

- "acquiring a client address and the user identifying information from the client apparatus when the authentication server receives the connection request from the client apparatus" (i.e. "memory 106, and at least one storage device") [column 8 line 47];
- "transmitting by the client apparatus to the authentication server a second connection authentication information generated by the client apparatus as user identification information together with a connection request" (i.e. "When the user signs onto the front-end server cluster 202, the central security process 222 transmits the user login data (e.g., username and password) to the policy server 204") [column 11 lines 11-14];
- "acquiring a client address and the user identifying information from the client apparatus when the authentication server receives the connection request from the client apparatus" (i.e. "When the user signs onto the front-end server cluster 202, the central security process 222 transmits the user login data (e.g., username and password) to the policy server 204") [column 11 lines 11-14];

but, Lander does not explicitly disclose,

- "associating the second connection authentication information with a connection server address of the connection server," although Fuh et al. do suggest storing client authorization information, as recited below;

- "transmitting the client address to the connection server address of the connection server when the user identification information is authenticated based on the second connection authentication information," although Fuh et al. do suggest sending and receiving source and destination IP addresses in the packets transmitted, as recited below;
- "transmitting the connection server address to the client apparatus," although Fuh et al. do suggest sending and receiving source and destination IP addresses in the packets transmitted, as recited below;
- "receiving by the client apparatus, independent of the connection server, the connection server address from the authentication server," although Fuh et al. do suggest sending and receiving source and destination IP addresses in the packets transmitted, as recited below;
- "transmitting by the client apparatus a first connection authentication information to the connection server address," although Fuh et al. do suggest receiving transmitted authentication information, as recited below;
- "receiving by the connection server the first connection authentication information from the client address," although Fuh et al. do suggest receiving transmitted authentication information, as recited below;
- "performing an authentication process by using the first connection authentication information transmitted from the client address," although Fuh et al. do suggest performing an authentication and authorization process, as recited below;
- "allowing the connection server to receive the first connection authentication information from the client address for a limited time period," although Fuh et al. do suggest permitting access, as recited below;

however, Fuh et al. do disclose,

- "storing client authorization information at the network device" [column 3 lines 5-6];
- "The fields include, among other things, values for source IP address and destination IP address of that packet" [column 10 lines 23-24];
- "Upon intercepting the HTTP packets, the firewall requests, from the client, authentication information such as username and password" [column 7 lines 48-50];
- "In response to receiving the authentication information, the firewall performs an authentication and authorization process" [column 7 lines 50-52];
- "In this context, "open a passageway" means that the firewall re-configures itself, in response to successful authentication, so that packets that would otherwise be barred are now allowed to pass" [column 7 lines 58-61];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "associating the second connection authentication information with a connection server address of the connection server" and "transmitting the client address to the connection server address of the connection server when the user identification information is authenticated based on the second connection authentication information" and "transmitting the connection server address to the client apparatus" and "receiving by the client apparatus, independent of the connection server, the connection server address from the authentication server" and "transmitting by the client apparatus a first connection authentication information to the connection server address" and "receiving by the connection server the first connection authentication information from the client address" and "performing an authentication process by using the first connection authentication information transmitted from the client address" and

"allowing the connection server to receive the first connection authentication information from the client address for a limited time period," in the invention as disclosed by Lander for the purposes of providing authentication based on multiple parts of information (i.e. address information, user identity, etc).

Claims 13 & 17:

Lander discloses a connection method using a network connection system including a client apparatus, an authentication server, and a connection server comprising,

- "storing by the authentication server a user name and a password which are encrypted by a first encryption method" (i.e. "memory 106, and at least one storage device") [column 8 line 47];
- "transmitting by the client apparatus to the authentication server a connection request and the user name and the password which are encrypted by the first encryption method" (i.e. "When the user signs onto the front-end server cluster 202, the central security process 222 transmits the user login data (e.g., username and password) to the policy server 204") [column 11 lines 11-14];
- "receiving by the authentication server the connection request from the client apparatus" (i.e. "When the user signs onto the front-end server cluster 202, the central security process 222 transmits the user login data (e.g., username and password) to the policy server 204") [column 11 lines 11-14];

- "acquiring a client address of the client apparatus and the user name and the password, which are encrypted by the first encryption method, as information identifying a user of the client apparatus" (i.e. "When the user signs onto the front-end server cluster 202, the central security process 222 transmits the user login data (e.g., username and password) to the policy server 204") [column 11 lines 11-14];
- "encrypting using a second encryption method a user name and a password input by a user" (i.e. "The user identifier may also be encrypted as an additional security precaution") [column 11 lines 46-48];

but, Lander does not explicitly disclose,

- "storing in a retention unit in the authentication server an association between both the encrypted user name and the encrypted password and a connection server address of the connection server," although Fuh et al. do suggest storing client authorization information, as recited below;
- "searching, by the authentication server, in response to receiving the information identifying the user of the client apparatus from the client apparatus, the retention unit for the information identifying the user of the client apparatus to determine the connection server address associated with the information identifying the user of the client apparatus," although Fuh et al. do suggest verification based on matching, as recited below;
- "transmitting the client address to the connection server address," although Fuh et al. do suggest sending and receiving source and destination IP addresses in the packets transmitted, as recited below;

- "receiving by the connection server the client address," although Fuh et al. do suggest sending and receiving source and destination IP addresses in the packets transmitted, as recited below;
- "switching, by the connection server, from a state in which authentication information is not allowed to be received from the client address. independent of the authentication server, to a state in which authentication information is allowed to be received from the client address, independent of the authentication server," although Fuh et al. do suggest reconfiguration to permit access, as recited below;
- "the switching occurring in response to the receiving of the client address," although Fuh et al. do suggest performing actions in response to receiving from a client, as recited below;
- "transmitting to the authentication server information indicating that the connection server has shifted to a connection wait state in which the connection server allows communication from the address of the client apparatus for a predetermined period," although Fuh et al. do suggest reconfiguration to permit access, as recited below;
- "transmitting, independent of the authentication server, to the connection server address the user name and the password which are encrypted by the second encryption method," although Fuh et al. do suggest receiving transmitted authentication information, as recited below;

- "performing, by the connection server, an authentication process by using the user name and the password which are encrypted by the second encryption method and are received by the connection server from the client apparatus," although Fuh et al. do suggest performing an authentication and authorization process, as recited below;
- "after a limited time period has elapsed since the connection server performs the switching, switching back from the state in which authentication information is allowed to be received from the client address, independent of the authentication server, to the state in which authentication information is not allowed to be received from the client address, independent of the authentication server," although Fuh et al. do suggest reconfiguration of access control for permitting/denying access, as recited below;

however, Fuh et al. do disclose,

- "storing client authorization information at the network device" [column 3 lines 5-6];
- "determining whether a source IP address of the client in the request matches information in a filtering mechanism of the network device; and if so, determining whether the source IP address matches the authorization information stored in the network device" [column 3 lines 48-52];
- "The fields include, among other things, values for source IP address and destination IP address of that packet" [column 10 lines 23-24];
- "In this context, "open a passageway" means that the firewall re-configures itself, in response to successful authentication, so that packets that would otherwise be barred are now allowed to pass" [column 7 lines 58-61];

- "Upon intercepting the HTTP packets, the firewall requests, from the client, authentication information such as username and password" [column 7 lines 48-50];
- "In response to receiving the authentication information, the firewall performs an authentication and authorization process" [column 7 lines 50-52];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "storing in a retention unit in the authentication server an association between both the encrypted user name and the encrypted password and a connection server address of the connection server" and "searching, by the authentication server, in response to receiving the information identifying the user of the client apparatus from the client apparatus, the retention unit for the information identifying the user of the client apparatus to determine the connection server address associated with the information identifying the user of the client apparatus" and "transmitting the client address to the connection server address" and "receiving by the connection server the client address" and "switching, by the connection server, from a state in which authentication information is not allowed to be received from the client address. independent of the authentication server, to a state in which authentication information is allowed to be received from the client address, independent of the authentication server" and "the switching occurring in response to the receiving of the client address" and "transmitting to the authentication server information indicating that the connection server has shifted to a connection wait state in which the connection server allows communication from the address of the client apparatus for a predetermined period" and "transmitting, independent of the authentication server, to the connection server address the user name and the password which are encrypted by the second encryption method" and "performing, by the connection server, an

authentication process by using the user name and the password which are encrypted by the second encryption method and are received by the connection server from the client apparatus" and "after a limited time period has elapsed since the connection server performs the switching, switching back from the state in which authentication information is allowed to be received from the client address, independent of the authentication server, to the state in which authentication information is not allowed to be received from the client address, independent of the authentication server," in the invention as disclosed by Lander for the purposes of providing authentication based on multiple parts of information (i.e. address information, user identity, etc).

11. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lander (US-7350229-B1) in view of Fuh et al. (US-6463474-B1) and in view of Johnson (US-20030163691-A1).

Lander discloses a computer readable medium storing a program causing a computer of a client apparatus to execute an access processing to a network system including an authentication server and a connection server comprising,

- "user identification information encrypted by the connection server with a first encryption method" (i.e. "The user identifier may also be encrypted as an additional security precaution") [column 11 lines 46-48];
- "encrypting the received user identification information with the first encryption method when the decrypted first and second information is correct" (i.e. "The user identifier may also be encrypted as an additional security precaution") [column 11 lines 46-48];

- "transmitting, to the authentication server, an access request and the received used identification information encrypted with the first encryption method" (i.e. "When the user signs onto the front-end server cluster 202, the central security process 222 transmits the user login data (e.g., username and password) to the policy server 204") [column 11 lines 11-14];

but, Lander does not explicitly disclose,

- "wherein, the authentication server includes (i) a first unit that acquires, from the connection server, an address of the connection server and," although Fuh et al. do suggest sending and receiving source and destination IP addresses in the packets transmitted, as recited below;
- "(ii) a first retention unit that stores the address of the connection server and the encrypted user identification information which are acquired by the first unit," although Fuh et al. do suggest storing client authorization information, as recited below;
- "the connection server includes a second retention unit that stores unique information which is unique to the client apparatus and the user identification information," although Fuh et al. do suggest storing client authorization information, as recited below;
- "the client apparatus includes a third retention unit that stores an address of the authentication server, first information and second information," although Fuh et al. do suggest several devices/apparatuses that are expected to have some form of storage in order to function, as recited below;

- "the access processing comprising: requesting a user to enter user identification information," although Fuh et al. do suggest requesting user identification input, as recited below;
- "receiving user identification information from the user," although Fuh et al. do suggest user entering identification input, as recited below;
- "generating unique information which is unique to the client apparatus in response to receiving the user identification information," although Fuh et al. do suggest user input identification information, as recited below;
- "judging whether the decrypted first and second information are correct," although Fuh et al. do suggest performing an authentication and authorization process, as recited below;
- "wherein the first information is generated by the connection server by encrypting predetermined information with the unique information as a key," although Johnson does suggest hashing/encrypting a first set of information, as recited below;
- "the second information is generated by the connection server by encrypting predetermined information with the user identification information as a key," although Johnson does suggest encrypting a second set of information, as recited below;
- "decrypting the first information stored in the third retention unit by using the generated unique information as a key," although Johnson does suggest decryption of previously encrypted information, as recited below;
- "decrypting the second information stored in the third retention unit by using the received user identification information as a key," although Johnson does suggest decryption of previously encrypted information, as recited below;

however, Fuh et al. do disclose,

- "The fields include, among other things, values for source IP address and destination IP address of that packet" [column 10 lines 23-24];
- "storing client authorization information at the network device" [column 3 lines 5-6];
- [FIG 3 illustrates a user client making a request to a firewall router and authentication server where it would not be unreasonable to expect a user client to have memory for storing information temporarily if not for an extended amount of time];
- "The login form is an electronic document that requests User 302 to enter username and password information, as shown by path 403" [column 11 lines 53-55];
- "To communicate the username and password information to Authentication Proxy 400, the user selects a "Submit" button 508" [column 11 lines 63-66];
- "A User 302 may enter username information in Username field 504 and may enter password information in Password field 506. To communicate the username and password information to Authentication Proxy 400, the user selects a "Submit" button 508" [column 11 lines 61-66];
- "In response to receiving the authentication information, the firewall performs an authentication and authorization process" [column 7 lines 50-52];

whereas, Johnson does disclose,

- "Once the user ID is received, the method computes a message digest of the user ID (step 215). This message digest is simply a binary number that is representative of the user ID. In this regard, the message digest may be a simple checksum or other processed value" [page 5 para 55 lines 11-13];

- "Once the encryption key is selected, the concatenated or otherwise combined message is encrypted using the access encryption key (step 240). Again, consistent with the scope and spirit of the invention, any of a variety of a known encryption methodologies or algorithms may be employed to perform this step" [page 5 para 62 lines 1-3];
- "Although not separately illustrated, it should be appreciated that the decryption process is simply the opposite of the encryption process that was illustrated in FIG. 3" [page 6 para 72 lines 1-3];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "wherein, the authentication server includes (i) a first unit that acquires, from the connection server, an address of the connection server and" and "(ii) a first retention unit that stores the address of the connection server and the encrypted user identification information which are acquired by the first unit" and "the connection server includes a second retention unit that stores unique information which is unique to the client apparatus and the user identification information" and "the client apparatus includes a third retention unit that stores an address of the authentication server, first information and second information" and "the access processing comprising: requesting a user to enter user identification information" and "receiving user identification information from the user" and "generating unique information which is unique to the client apparatus in response to receiving the user identification information" and "judging whether the decrypted first and second information are correct" and "wherein the first information is generated by the connection server by encrypting predetermined information with the unique information as a key" and "the second information is generated by the connection server by encrypting predetermined information with the user

identification information as a key" and "decrypting the first information stored in the third retention unit by using the generated unique information as a key" and "decrypting the second information stored in the third retention unit by using the received user identification information as a key," in the invention as disclosed by Lander for the purposes of providing authentication based on multiple parts of information (i.e. address information, user identity, etc) while utilizing multiple encryption steps for improved security.

Response to Arguments

12. Applicant's arguments with respect to claims 1-3, 5-7, 10, & 13-18 have been considered but are moot in view of the new ground(s) of rejection as necessitated by the applicant's amendments.

13. Applicant's arguments, see pages 17-21, filed 09/09/2008, with respect to the rejection(s) of claim(s) 9, 11, & 12 under 35 U.S.C. 102(e) and 35 U.S.C. 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of a different interpretation of the previously applied reference and in view of newly found prior art references.

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to the applicant's disclosure.

a. Henry et al. (US-6971005-B1 and US-7069433-B1) – virtual single account client [covers some similar aspects with respect to the protection of remote access and generation of encryption information (i.e. key)]

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/OAL/
12/05/2008

/Carl Colin/
Primary Examiner, Art Unit 2436